面向健康医疗大数据安全保护的医疗区块链模型构建

■ 李洪晨[1] 马捷[1,2] 胡漠[1]
[1] 吉林大学管理学院 长春 130022 [2] 吉林大学信息资源研究中心 长春 130022

摘 要：[目的/意义]在医疗信息化迅速发展过程中，医疗大数据信息安全保护存在数据丢失、难以共享等问题。为了更好地对健康医疗大数据进行保护，本文构建面向健康医疗大数据安全保护的医疗区块链模型，解决健康医疗大数据集中存储、不可追溯、易受攻击等问题，为进一步推动区块链技术在健康医疗领域的应用提供方案。[方法/过程]构建基于区块链技术的健康医疗大数据信息安全保护模型和系统架构，通过PBFT共识算法保证医疗区块链数据的不可篡改，通过非对称加密技术保证个人医疗信息的安全性，通过激励机制鼓励各节点加入医疗区块链。[结果/结论]相对于传统的医疗信息保护方法而言，面向健康医疗大数据安全保护的医疗区块链模型具有数据可追溯、防篡改和信息平等共享、安全可信等优势，可以更好地推动健康医疗数据化的发展。

关键词：健康医疗大数据 区块链去中心化 信息安全保护 PBFT算法
分类号：G203
DOI：10.13266/j.issn.0252-3116.2021.02.004

医疗数据化、信息化的飞速发展为人们保健就医提供了便利，但与此同时产生的海量医疗保健数据存储、利用和安全性问题也愈发引起人们的关注。近年来，健康医疗行业发生了多起堪称“毁灭性”的数据丢失、泄露事件。例如美国第二大医疗保险服务商Anthem信息系统被黑客攻破，超过7 800万客户信息泄露，美国健康保险公司“Premera Blue Cross”的信息系统遭到网络攻击，造成了1 100万客户信息泄露[1]。德国Greenbone Networks公司的专家发现，超600个未受保护的服务器被暴露在互联网上，这些服务器被暴露的内容中包含大量医疗放射图像。这其中中国有14个未受保护的PACS服务器系统，泄露279 000条数据记录[2]。当前医疗保健信息系统存在的一些漏洞，为黑客提供了可乘之机，网络窃密、数据丢失、黑客入侵事件频繁发生，健康医疗大数据频涉信息安全危机。数据安全问题不是健康医疗领域特有的问题，但由于健康医疗大数据具有高度敏感性和隐私性，包含了公民最为隐密的身体、疾病信息，以及个人生活轨迹、住所、医疗保险、财产等信息，个人健康信息一旦发生数据泄露，造成的后果极其严重。

2019年10月24日，中共中央政治局首次就区块链技术发展现状和趋势进行学习，学习中提出的四个“要”为区块链技术如何给社会发展带来实质变化指明了方向[3]。其中第一“要”是要探索民生领域的区块链技术应用场景，积极推进区块链技术与健康医疗领域相结合。区块链技术中的数据存储方式和区块产生方式使存储在区块链中的数据具有无法被篡改、可追溯、保障交易隐私、具有时序性的特点，这些特点使区块链天然带有极强的金融属性、交易属性。而区块链技术提供的保障信息安全完整、防泄漏服务，使其与金融领域有更好的结合。健康医疗和金融虽不相同，但在信息交流复杂、信息量庞大、信息交流参与方众多的健康医疗领域，信息在系统里需要进行多次交换、添加和读取，这种信息转手与金融领域里的交易相似，区块链为健康医疗大数据信息安全问题提供了一条新的解决思路。

1 文献回顾

健康医疗大数据是指包括自然人身体健康状况、疾病防治及医疗行为的具有隐私属性的全部信息[4]。既包括能够直接表明个人身份的隐私信息如年龄生日、姓名、联系方式和身份证号等，也包括在医疗过程

作者简介：李洪晨(ORCID:0000-0002-1602-9230)，硕士研究生；马捷(ORCID:0000-0002-1471-2143)，教授，博士，博士生导师，通讯作者，E-mail:m-l-j-1@163.com；胡漠(ORCID:0000-0003-1605-9755)，博士研究生。
收稿日期：2020-05-19 修回日期：2020-10-04 本文起止页码：37-44 本文责任编辑：王传清

中记录的患者的身体特征、疾病情况、身体健康情况、药物过敏情况和家族病史等。

1.1 医疗大数据信息安全保护研究

在现阶段,医疗机构大数据的管理制度和信息系统的数据保护技术未能满足当前健康医疗大数据信息安全保护的需要,健康医疗信息存在数据易丢失[5]、易泄漏[6-7]、难共享[8]等问题。

国内外针对健康医疗大数据信息安全保护的研究主要围绕基于访问控制的技术、基于数据加密的技术和利用规则引擎技术展开。孙佰利等通过分析健康医疗大数据的特点,提出的利用加密算法和密钥对数据进行加密存储实现了数据源层面保护敏感信息不被泄露的目的[9];I. Blanquer 等在医学成像平台上利用本体进行自动授权,加强对医疗信息的保护和存储效率[10];刘逸敏等通过研究关系数据库中细粒度访问控制模型,分析模型在医院数据应用场景下存在的问题,并探求具体的解决方案[11];贾瑞龙等提出了一种新的具有显著计算增益的细粒度访问结构 G-CP-ABE,在一定程度上提高了医疗数据的保密性和数据访问的隐私性[12]。

随着健康医疗大数据时代的来临,医疗大数据格式的多样性和数据量的迅速增长等特点对信息安全保护带来新的挑战,当前的信息安全保护方案都依赖于一个完全可信的、独立的第三方来保证交互的可靠性。一旦单一的第三方信任机构遭到攻击,其所保护的信息也都不再安全。仅从技术方面未能从根本上解决当前出现信息的泄露和丢失现象,医疗信息保护需要一种全新的、去中心化的方式来实现,因此提出基于区块链技术的健康医疗大数据信息安全保护策略。

1.2 健康医疗大数据医疗区块链研究

国内基于区块链技术对健康医疗大数据信息安全保护的研究还在起步阶段。王辉等构建了去中心化的医疗数据存储系统、改进的 PBFT 共识算法以及数据交互系统的架构,实现了医疗数据的安全、可追溯和防篡改[13]。

国外的研究相对成熟, E. Andy 指出区块链技术可以帮助用户可靠地收集和保存有关研究活动的数据资源,通过创建不损坏的数据线索安全地记录发布决策来增强大数据资源的可重复性和数据开发过程[14]。S. Patel 等通过跨域图像共享的框架,将区块链作为分布式数据存储账本,允许放射学研究和患者定义不同的数据的访问权限[15];C. Esposito 等研究了使用区块链技术保护保存在云中的医疗数据,解决了使用常规加密语言和访问控制而出现的问题[16];H. Li 提出了一种新颖的基于区块链的医疗数据保存系统(Data Preservation System),该方法可以保证数据的原始性和可检验性,即使数据被盗,也无法得知用户相关的信息[17]。M. Waal 等提出针对当前新冠疫情所涉及的数据信息,利用区块链的技术方法促进不同节点间数据资源的共享行为,并打破掣肘持续性共享的壁垒,进而推动数据资源的研发应用进展[18]。

基于目前区块链技术对健康医疗大数据信息安全保护的研究多仅从数据存储系统的层面进行,未将患者、医院和其他相关机构如乡镇卫生院、健康档案、保险公司、公安和科研机构等相关节点纳入模型的范围内,本文从机构层面出发构建面向健康医疗大数据安全保护的医疗区块链模型。

2 健康医疗大数据及区块链技术特征

2.1 健康医疗大数据类型及特征

健康医疗大数据泛指所有与生命健康相关的数据[16]。从数据的来源来看,主要产生自患者、医院、体检机构、第三方诊疗等,与其他行业大数据相比数据的来源更广;从数据的覆盖范围看,数据涵盖用户出生、疫苗注射、入学和工作体检、医院就诊住院、运动、睡眠、直到死亡整个生命周期产生的所有相关数据,健康医疗大数据具有海量性和隐私性的特点;从数据的传输过程来看,健康医疗大数据在患者、医保商保机构、卫生监管部门、医院、药企和实验室之间传输,且各组织相互独立,因此数据传输的参与节点相较于金融、制造业等领域更多且更为独立。

2.2 医疗区块链技术特征

医疗区块链是一个可以以时间为记录顺序进行数据管理并保证数据不可篡改的分布式医疗信息数据库,其数据结构是由以时间顺序排列的数据块组成,每个数据块都包含了一段时间内用户的健康医疗信息,并在区块上加盖时间戳和指向上一个区块的指针。针对健康医疗大数据信息来源和交易的信任问题,医疗区块链[19]系统各节点无需了解其他节点的背景资料,也不需要借助第三方机构的担保或保证,从而保障了系统对医疗数据传输的活动进行记录、传输、存储是可信的[20]。分布式账本要求医疗信息交易记账由分布

在不同地方的不同节点共同记录，每个参与节点都要存储完整的医疗账目，由此保障医疗信息交易的合法性。与传统的医疗信息存储相比，医疗区块链的分布式账本独特性主要体现在以下3个方面：

（1）分布式记账。区块链每个节点都按照块链式结构存储完整的医疗数据，让所有节点都能参与记录和验证，构建的协议机制让系统内每个节点在参与记录的同时也可以验证其他节点记录医疗信息的正确性。只有当系统内超过半数节点同时认为该条记录正确时，该条记录的真实性才会得到医疗区块链系统的认可，记录医疗数据才允许被写入医疗区块中。

（2）分布式存储。医疗区块链内各个节点存储都是相互独立的、地位等同的，共识机制保证各节点存储的一致性，从而确保没有任何一个节点可以单独记录账本数据，避免了单一记账人被控制或部分节点被攻击致使数据丢失的可能性。当医疗区块链上的节点数量足够多时，理论上如若不是超过半数多节点被破坏，健康医疗账目就不会丢失，从而提高了账目数据的安全属性。

（3）分布式传播。医疗区块链中每一笔新信息交易都采用分布式的结构，按照开源的P2P网络层协议进行传播，医疗信息通过分布式传播由某个节点被直接发送给系统内其他的所有节点。通过分布式记账、分布式存储和分布式传播三大特点可以确保没有哪个个人或者组织可以控制这个医疗系统，在大多数参与者达成共识后即可共同构建医疗区块链数据库。

区块链的共识机制可以很好地解决健康医疗大数据传输节点多且相对独立的问题，共识机制功能是为所有医疗区块链参与节点之间就怎么达成共识、如何去认定一个记录的有效性提供标准。这既是认定的手段，也是防止篡改的手段，遵循“人人平等”和“少数服从多数”原则。“人人平等”是当节点满足条件时，所有节点都平等地享有提出共识结果、直接被其他节点认同后并最后有可能成为最终共识结果的权利。“少数服从多数”原则决定了只有在控制了系统内超过51%的参与节点的情况下，才有可能伪造出一条不存在的健康医疗记录。当加入医疗区块链的节点足够多的时候，这基本上不可能，从而杜绝了医疗数据造假的可能。

区块链提出了4种不同的共识机制[18]，以满足不同的应用场景效率和安全之间的平衡需求：①POW（Proof of Work）为比特币共识算法，要求算力较大；②POS（Proof of Stake）是以太币共识算法，对算力的依赖相对较小；③DPOS（Delegated Proof of Stake）在加强区块链的安全性的同时进一步削减对算力的浪费；④PBFT（Practical Byzantine Fault Tolerance）在保证灵活性和安全性的前提下提供了(n-1)/3的容错性。本文研究利用区块链技术实现健康医疗大数据信息安全保护，需要在提供高数据处理量的同时尽可能的低时延，因此选择PBFT算法作为共识机制。

医疗区块链内用户健康医疗大数据安全性增强主要通过以下3种方式实现：

（1）医疗区块链系统是由其中所有参与的节点共同更新、维护的，这要求系统内每一个参与节点都拷贝当前最新的完整医疗数据库，单个节点甚至多个节点对医疗数据库的篡改不能改变其他节点拷贝的医疗数据库，只有控制整个医疗区块链系统中超过51%的参与节点同时修改同一内容时，其余节点保存的医疗数据库才会被修改，而这在节点数量巨大时几乎不可能发生。医疗区块链中每一笔传输的医疗信息区块都通过密码学技术与相邻两个医疗区块串联，因此可以追溯到任何一笔信息传输的时间和地点，这可以从数据的层面保证每一份录入的用户医疗数据不被个人或机构更改。

（2）每个参与节点可以将医疗区块链系统需要的信息生成私钥，向需要查看该医疗信息的其他节点发送公钥，非对称加密技术保证即使拥有公钥，也不能反推出私钥，从技术层面保证每个节点上的隐私不被泄漏。新的节点加入医疗区块链必须验证，若是使用私钥发布了虚假医疗消息，经查实后将被踢出医疗区块链系统，保证医疗组织的长期稳定性和安全性。

（3）通过时间戳能够证明一份医疗数据在某个特定时间之前已经存在且完整，时间戳即一个字符序列，可以标识某一医疗信息发布、修改和查看的具体时间。医疗区块链上的每一个区块都带有时间戳，它记录健康医疗信息录入的时间，通过时间纬度可以查询某节点的医疗数据和数据记录的时间顺序，这有助于对用户病例和个人相关信息进行追溯[13]。

3 面向健康医疗大数据安全保护的医疗区块链模型

健康医疗大数据信息安全保护由医疗信息的生成和使用方、医疗信息交换中介和信息交换的监督方三方构成，由此面向健康医疗大数据安全保护的医疗区

块链模型构成要素包括监管中心、信息聚合机构、信息交换实体三部分,如图 1 所示:

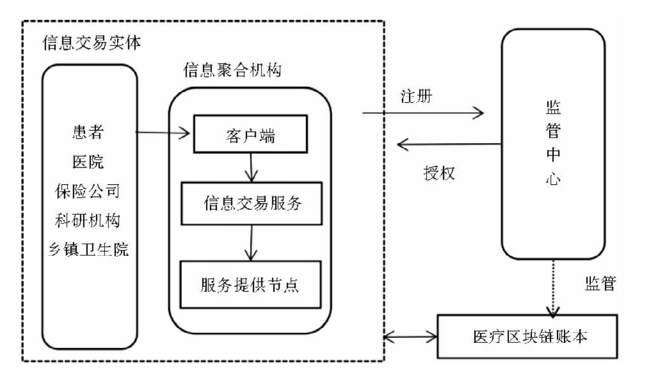


图 1 面向健康医疗大数据安全保护的医疗区块链模型

3.1 医疗区块链模型构成

在信息安全保护模型中,参与信息交换的实体包括患者、医院和其他相关机构如乡镇卫生院、健康档案、保险公司、公安和科研机构等。信息交换实体可以根据自己的意愿和实际需求,选择赋予医院和其他相关机构访问和使用权限。患者在诊疗后通过自己的私钥对个人所产生的医疗健康数据进行签名,以确认数据的准确性和私密性,每条医疗数据包含数据所有者的公钥(Patient PK)、医疗元数据和数据摘要[21]。

如图 2 所示,患者的健康医疗数据包含医疗元数据块和数据摘要块。数据摘要块包括时间戳(Timestamp)、医生公钥(Doctor Pk)、医疗数据的描述(Data Description)和医疗数据的类型(Data Type)。医疗元数据块包括医生公钥、文件路径(Path To File)和 hash 值等。为了生成有效医疗区块需要将组装的备选医疗区块进行 hash 运算,算出一个合适的随机数,每个医疗区块中都有一个难度系数,通过难度系数可以推算出一个目标值。医疗区块的头部中有一个随机字符串,每次医疗信息保存需要对头部进行 hash 计算,如果 hash 结果小于目标值,那么该区块被认证为有效区块,可以进行后续广播区块的操作;如果 hash 结果不小于目标值,那么该区块将被认为是无效区块,修改随机字符串后重新计算 hash 值。

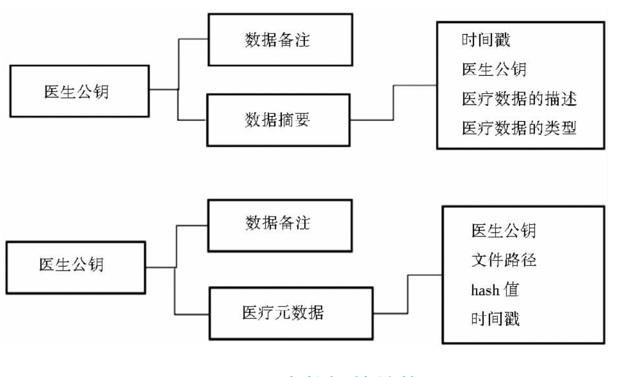


图 2 医疗数据的结构

医院通过医疗区块链将患者产生的数据上传至区块链和分布式数据库,从而确保了数据的不可篡改性;保险公司、科研机构等可在患者授权的情况下通过公钥检索患者的医疗健康数据,为保险理赔、科研活动提供数据支持。

信息聚合机构作为信息交换的中介,保存信息交换的完整区块链数据,并为医院、患者、其他相关机构通过通讯服务。每次进行信息传输都要向最近的信息聚合机构发送传输请求,信息聚合机构对请求进行核实,并向所有的信息聚合机构广播这一操作。

监管中心作为医疗信息传输的监管部门,对信息聚合机构、信息交换实体授权的同时,对传输的医疗数据进行监管。基于区块链技术的健康医疗大数据信息安全保护模型,运用区块链技术来实现现有医疗管理体系无法达成的、以用户为中心的、高度机密的医疗数据保护体系,在推进不同医疗机构间、跨数据平台间的医疗大数据共享的同时保护用户的医疗数据不被泄漏。

3.2 医疗区块链层次及其关系

面向健康医疗大数据安全保护的医疗区块链由健康医疗数据层、医疗链网络层、医疗共识层、用户参与激励层、医疗系统合约层和医疗链应用层 6 个层次构成[22],如图 3 所示:

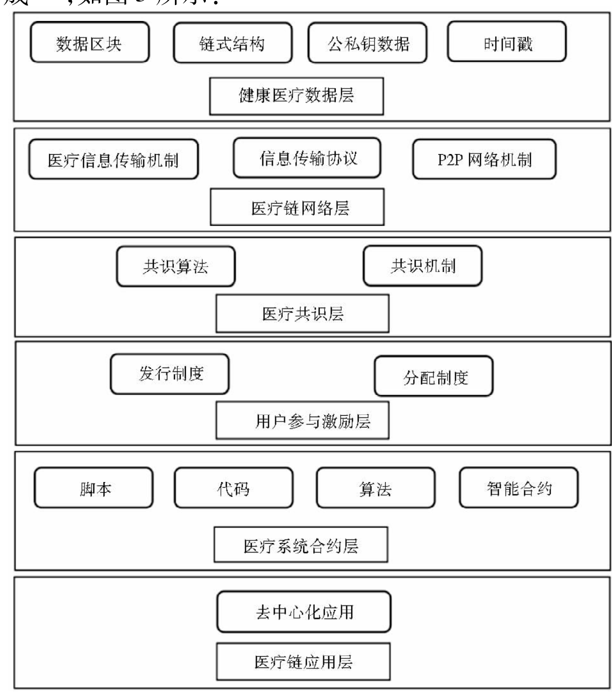


图 3 面向健康医疗大数据安全保护的医疗区块链层次

3.2.1 健康医疗数据层

健康医疗数据层是整个医疗区块链系统中最底层的数据结构，随着健康医疗数据交易的不断发生，医疗数据交易链内的各节点之间产生的信息量必然增大，各节点之间产生的流动必然加快。针对健康医疗系统的特点，各节点在医疗区块链上体现的信息为数据区块。在交易数据下，各节点自身的状态数据主要是为了时刻记录信息交易过程中医疗信息的各种状态，医疗信息管理人员可以随时查看。每一次信息交易完成的交易数据，会在一段固定时间内通过哈希算法来生成相对应的哈希值[23]。如交易信息量小、时间间隔较短可以保留所有信息交易的哈希值，并将哈希值链接医疗区块头中的 Merkle 根上。如健康医疗链中信息交易数量庞大，则需要将原记录的 hash 值进一步计算，反复迭代，直到满足医疗区块存储要求后将最后一代哈希值链接到 Merkle 根中。医疗区块头则记录了当前版本、前一区块地址、时间戳、Merkle 根以及交易医疗信息数量的信息，将前一区块地址和当前区块的数据哈希值链接，可以将各个医疗区块之间相互连接形成一条可以从最新区块追溯到最新的医疗数据区块的完整主链，图 4 展示了医疗信息交易区块建立过程：

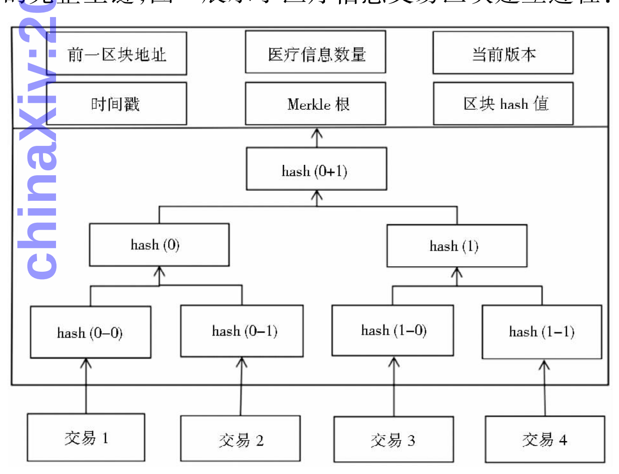


图 4 医疗信息区块结构

3.2.2 医疗链网络层

医疗链网络层由各级医院、乡镇卫生院、健康档案、保险公司、卫生监管部门和科研机构等节点构成。由于当前健康医疗大数据一般保存在三甲医院和高水平的医疗科研机构内，因此将三甲医院和高水平研究机构节点设为共识节点，进行医疗区块的组装、生成和广播，其余医院节点不参与医疗区块链的记账，仅需要同步整个账本和将患者签名的健康医疗数据上传至上级医院。由于链内的校验和新区块的认可都是由信息传输机制和信息传输协议保证，这决定了区块链的实质是一个机会均等的 p2p 网络，各节点之间机会均等、责任共但。

3.2.3 医疗共识层

医疗共识层是医疗区块链的核心技术，其主要功能是让高度分散的节点在去中心化的医疗区块链网络中高效地针对区块数据的有效性达成共识，以高效地解决各节点之间信任问题。该模型采用 PBFT 共识算法，在提高数据准确性的同时尽量降低对算力的依赖，更好地适应健康医疗大数据数据量大、即时性强的特点。

3.2.4 用户参与激励层

当医疗信息发布主体和其他信息接收机构遇到利益不一致时，用户参与医疗区块链的积极性就会大大降低[24]。本文通过信用积分模型[25]鼓励用户参与医疗区块链，当用户在医疗区块链上共享医疗信息时获得相应收益，当医疗信息使用者获取医疗信息时支付相应成本，以此保证面向健康医疗大数据安全保护的医疗区块链模型中的利益分配是均等的。为实现模型利益均等分配，对参与医疗信息共享区块链建立的节点提供初始积分，此后节点提供有效医疗信息获得积分奖励，提供不实医疗信息受到积分惩罚。

本文构建的信用积分模型可以使用户在平台上存储和发布个人健康医疗信息时，无论作为信息提供者还是信息的使用者，都对支付成本和收益进行公平的核算，以此保证医疗区块链各节点的利益分类是均等的。通过节点在医疗信息存储和共享过程中的表现对其信用进行打分，利用信用积分可以获得会员服务、兑换现金等，使得各节点在信息共享过程中能够各取所需，在满足个人理性需求的前提下促进健康医疗数据的保护和挖掘，并且在医疗区块链上可以根据信用积分体制建立合理便捷的退出机制，使得各类节点可以根据自己的意愿随时退出，消除了用户的后顾之忧。

3.2.5 医疗系统合约层

医疗系统合约层由各类脚本、代码、算法以及智能合约组成。智能合约要求医疗数据收集、储存和利用的参与者签署并以代码的形式附在医疗区块链或令牌上，从而实现区块链账本记录功能。智能合约中封装了触发合约的各种条件，系统自动判断是否达到合约条件，一旦达到某个确定的合约条件，系统立即执行，

无需第三方确认，这从源头确保合约的执行不受任何外界因素的干扰，所以说合约层是区块链去信任的技术基础。例如当医院和患者达成医疗信息交易智能合约后，该合约就以代码的形式嵌入医疗区块链中，系统自动判断上传的数据是否符合合约条件，若符合要求即判断合约立即生效。

3.2.6　医疗链应用层

医疗链应用层规定了医疗区块链的应用范围，该层主要负责医疗信息储存和信息查询及验证。健康医疗大数据隐私信息保护区块链中交易的信息都带有时间戳和信息验证记录，应用层就是通过保存交易信息及其相关信息避免数据丢失。由于交易的信息本身及其时间戳和验证记录都得以保留，任何时候接受建设医院、科研机构、地方诊所或政府检查都可以快速地定位到信息位置，证明信息真实存在。

4　面向健康医疗大数据安全保护的医疗区块链模型运行

信息聚合机构由客户端、信息交易服务器和服务提供节点构成。客户端负责发送医疗信息、发送使用信息请求、接收信息及评价信息，相较于金融、工业等领域区块链，医疗区块链参与节点众多、各节点相互独立且不同节点数据量需求差异巨大，因此根据健康医疗大数据不同用户的使用目的和所需数据量，将医疗区块链客户端设计为用户级客户端、医生级客户端和机构级客户端 3 种类型，以提升该医疗区块链模型的应用可行性：①用户级客户端：该类型是网页的模式，患者在就诊结束后通过用户客户端申请数据记录上传，当患者再次就诊时可以授权查询获得自己的历史记录，该客户端的主要目的是为患者提供简单自我查阅的服务。②医生级客户端：该类型不保存患者的健康医疗数据，仅为医疗机构提供查询接口并对患者数据进行授权操作。③医院级客户端：该类型客户端需要存储健康医疗大数据，并为医保商保机构、卫生监管部门、药企科研机构等提供对外服务。

信息交易服务器主要负责从客户端接受医疗信息、使用信息请求和评价信息并为客户端和服务提供节点之间提供验证服务，服务提供节点用于存储验证通过的区块链信息和发送需求信息区块。详细的医疗信息交易过程见图 5。

（1）信息生产流程。用户生成个人健康医疗数据

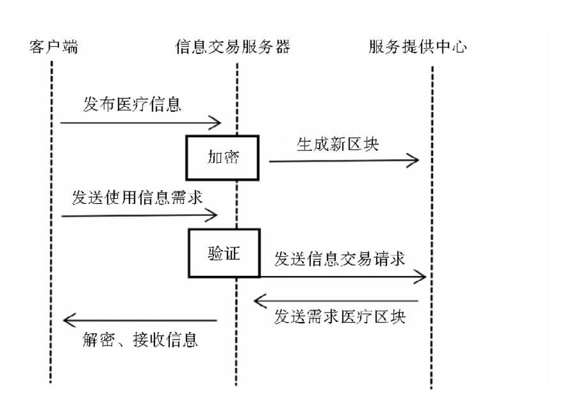


图 5　模型运转流程

前，首先需要进行新用户注册，监管中心做为第三方证书授权机构，接收每个新用户向监管中心提交的相关信息，经过其核验后授权给用户数字签名以及自己专属的公钥和私钥。私钥 Patient SK 和公钥 Patient PK 由监管中心根据用户提交的姓名、年龄、身份证号等相关信息使用非对称加密算法生成，数字签名 sign 由生成私钥 Patient SK 对用户的公钥 Patient PK 进行加密形成。新用户完成注册后即成为该区块链的一个合法节点，其数字签名 sign 合法性可通过其他用户的监管中心公钥 PK 来验证。当新用户要参与信息传输时，需要将自己的账户上传到信息聚合机构，从中下载最新的传输数据，同步区块头数据。此举极大地减少了用户接收和存储数据的负担，不需将信息聚合机构中已经存储了的所有区块链数据都存储在用户账号中。

（2）信息传输流程。患者以智能合约的形式向本地信息聚合商发送个人医疗信息，对传输的医疗文件进行加密，经信息交易服务中心执行 PBFT 共识算法，区块链中的主节点将一段时间内接收到的医疗信息单打包发送给从节点来验证，从节点对提取出医疗信息的非对称加密公钥进行验证，验证通过则计入医疗区块链；若验证出现错误，则说明医疗信息已被篡改，退回该个人医疗信息并不记入医疗区块，同时将验证错误的结果返回给用户。

（3）信息验证流程。账户选择完毕，信息交易服务中心将请求信息打包，并广播到所有本地信息聚合商中。信息交易服务中心选择交易账户，信息交易双方匹配成功后，信息需求方从本地信息聚合商处接收信息提供方所提交的合约，并产生新的合约。信息提供方对交易记录进行验证并进行数字签名，将交易记录上传给信息聚合机构进行验证。通过验证后用户在医疗区块链找查找关键词，使用可搜索加密算法生成

陷门,用户生成查询账单后发送查找请求给区块链数据库上的共识节点,区块链数据库共识节点接收到查询请求后,从查询请求中提取陷门,通过可检索的加密算法进行匹配检索用户需要的结果。用户接收到返回的查询结果后,使用密钥对加密的数据进行解密查看明文医疗信息。

5 结语

本文具体研究了面向健康医疗大数据安全保护的医疗区块链模型使用的区块链技术、模型的构成要素和层次关系及模型的运作流程,构建了医疗区块链模型,通过该模型增强医疗机构之间、医疗机构和其他相关机构间的数据共享与合作,提高医疗数据的准确性和利用率,患者有效治疗的可能性更高,医疗体系的运作成本、患者的诊疗成本也会降低。但由于当前区块链技术发展的不成熟,区块链的底层设施很不完善,面对海量的健康医疗大数据去中心化的存储和计算需要花费大量的时间,而医疗场景里对数据时效性的要求极高,如何提高医疗区块链的效率是需要继续研究的课题。

参考文献:

[1] 美国第二大医疗保险公司 Anthem 遭黑客入侵,近 8000 万用户数据泄露[EB/OL]. [2020－02－11]. https://www.freebuf.com/news/60134.html.
[2] 全球 7.37 亿医疗数据泄露,涉及 2000 多万人,波及 52 国[EB/OL]. [2020－02－19]. https://www.infoq.cn/article/8VZ8aVetNvRQ2VCmHl4u? utm_source=tuicool&utm_medium=referral.
[3] 新华网. 习近平在中央政治局第十八次集体学习时强调 把区块链作为核心技术自主创新重要突破口 加快推动区块链技术和产业创新发展[EB/OL]. [2020－02－19]. http://www.xinhuanet.com/politics/leaders/2019-10/25/c_1125153665.htm.
[4] 洪建,李锐,徐王权. 医疗健康数据隐私保护技术综述[J]. 中国数字医学,2015,10(11):83－86.
[5] 王天屹,刘爱萍. 大数据环境下医疗数据隐私保护对策研究[J]. 信息技术与网络安全,2019,38(8):28－32.
[6] 赵汉青,罗杰,王志国. 互联网医疗健康服务模式中的信息安全挑战[J]. 中国数字医学,2019,14(8):92－93,117.
[7] 李志强, 康立军, 王文翠. 面向医疗信息的大数据安全管理策略探究[J]. 计算机安全, 2014(4):84－86.
[8] 许岩. 论引入区块链技术促进"互联网+医疗健康"发展[J]. 中国医疗管理科学,2018,8(4):40－44.
[9] 孙佰利,米海英,李玲. 健康医疗大数据的信息安全保护策略初探[J]. 现代信息科技,2019,3(19):156－158.
[10] BLANQUER I, HERNNDEZ V, SEGRELLES D, et al. Enhancing privacy and authorization control scalability in the grid through ontologies[J]. IEEE transactions on information technology in biomedicine, 2009, 13(1):16－24.
[11] 刘逸敏,王志勇,乔晋,等. 细粒度访问控制技术在医疗数据库中的应用与展望[J]. 中国数字医学,2008,3(11):45－49.
[12] 贾瑞龙,曹亚州,苗俊青,等. 基于改进 CP-ABE 模型的医疗数据隐私保护管理设计与应用[J]. 计算机测量与控制,2020,28(1):200－204,209.
[13] 王辉,刘玉祥,曹顺湘,等. 融入区块链技术的医疗数据存储机制研究[J/OL]. 计算机科学:1－9. [2020－03－19]. http://kns.cnki.net/kcms/detail/50.1075.TP.20200225.1400.006.html.
[14] ANDY E. Could bitcoin technology help science? [J]. Nature, 2017, 552(7685): 301－302.
[15] PATEL S, VISHAL M. A framework for secure and decentralized sharing of medical imaging data via blockchain consensus[J]. Health informatics journal, 2018, 25(4):1398－1411.
[16] ESPOSITO C, SANTIS A D, TORTORA G, et al. Blockchain: a Panacea for healthcare cloud-based data security and privacy? [J]. IEEE cloud computing, 2018, 5(1):31－37.
[17] LI H, ZHU L, SHEN M, et al. Blockchain-based data preservation system for medical data[J]. Journal of medical systems, 2018, 42(8):141－154.
[18] WAAL M, RIBEIRO C, MA M, et al. Blockchain-facilitated sharing to advance outbreak R&D[J]. Science, 2020, 368(6492): 719－721.
[19] 许培海,黄匡时. 我国健康医疗大数据的现状、问题及对策[J]. 中国数字医学,2017,12(5):24－26.
[20] 胡漠,马捷. 信息协同视角下无边界化智慧政务推进机制研究[J]. 情报资料工作,2019,40(1):44－51.
[21] 何蒲,于戈,张岩峰,等. 区块链技术与应用前瞻综述[J]. 计算机科学,2017,44(4):1－7,15.
[22] 薛腾飞,傅群超,王枞,等. 基于区块链的医疗数据共享模型研究[J]. 自动化学报,2017,43(9):1555－1562.
[23] 袁勇,王飞跃. 区块链技术发展现状与展望[J]. 自动化学报,2016,42(4):481－494.
[24] 胡漠,马捷. 异构区块链网络视域下智慧养老多元信息协同模式研究[J]. 图书情报工作, 2020, 64(7):110－118.
[25] 石进,邵波,苗杰. 基于区块链的中小企业竞争情报共享平台研究[J]. 图书情报工作,2019,63(20):112－120.

作者贡献说明:

李洪晨:撰写论文,修改论文;
马捷:确定论文选题及整体研究框架,修改论文;
胡漠:修改论文。

Construction of a Medical Blockchain Model for the Security Protection of Healthcare Big Data

Li Hongchen[1] Ma Jie[1,2] Hu Mo[1]
[1] School of Management, Jilin University, Changchun 130022
[2] Resources Research Center, Jilin University, Changchun 130022

Abstract: [Purpose/significance] In the rapid development of medical informatization, traditional medical information security protection has problems such as data loss and difficulty in sharing. In order to protect health and medical big data better, this paper proposes the construction of a medical blockchain model for the security protection of healthcare big data to solve the problems of centralized storage, untraceability, and vulnerability, and provides solutions for further promoting the application of blockchain technology in the field of health care. [Method/process] This paper built a health care big data information security protection model and system architecture based on blockchain technology, ensured that the medical blockchain data can not be tampered through the PBFT consensus algorithm, and ensured the safety of personal medical information through asymmetric encryption technology, then encouraged all nodes to join the medical blockchain through an incentive mechanism. [Result/conclusion] Compared with the previous medical information protection methods, the health care big data information security protection model based on blockchain technology has the advantages of data traceability, tamper resistance, equal sharing of information, security and credibility, etc. It can promote the development of health care digitalization better.

Keywords: health and medical big data　blockchain decentralization　information security protection　PBFT algorithm

《图书情报工作》杂志社发布出版伦理声明

为加强和增进学术论文写作、评审和编辑过程中的学术规范、科研诚信与学术道德建设,树立良好学风,弘扬科学精神,坚决抵制学术不端,建立和维护公平、公正、公开的学术交流生态环境,《图书情报工作》杂志社(包括《图书情报工作》《知识管理论坛》两个期刊编辑部)结合两刊实际,特制订出版伦理声明并于 2020 年 2 月正式发布。

该出版伦理声明承诺两刊将严格遵守并执行国家有关学术道德和编辑出版相关政策与法规,规范作者、同行评议专家、期刊编辑等在编辑出版全流程中的行为,并接受学术界和全社会的监督。共包括三大部分,总计十五条,分别为:一、作者的出版伦理(①学术论文是科学研究的重要组成部分;②学术不端是学术论文的毒瘤;③作者是学术论文的主要贡献者;④ 作者署名体现作者的知识产权与学术贡献;⑤学术论文要高度重视知识产权与信息安全;⑥参考文献的规范性引用是学术规范的重要表征;⑦要高度重视研究数据与管理的规范性;⑧建立纠错与学术自我净化机制)。二、同行评议专家的出版伦理(⑨同行评议是论文质量的重要控制机制;⑩评审专家应遵守论文评审的相关要求;⑪评审专家要严格遵循相关的伦理指南和行为准则)。三、编辑的出版伦理(⑫编辑应成为学术论文质量的守护者;⑬编辑应在学术道德建设中发挥监控作用;⑭编辑要成为遏制学术不端的最后屏障;⑮对学术不端实行“零容忍”)。

全文请见:http://www.lis.ac.cn/CN/column/column291.shtml

(本刊讯)